XXXII SEMINARIO INTERNACIONAL DE SEGURIDAD Y DEFENSA: "AMENAZAS DESDE EL CIBERESPACIO"

Inteligencia en el ciberespacio

En primer lugar, quiero **agradecer** a la Asociación de Periodistas Europeos, y especialmente a su Secretario General, Miguel Ángel Aguilar, **la invitación** a participar en este Seminario Internacional de Seguridad y Defensa. Gracias por el tesón que demostráis en la celebración, año tras año, de este encuentro. Treinta y dos ediciones es tiempo más que suficiente para que valoremos muy positivamente el interés de estas convocatorias, siempre tan bien y tan cuidadosamente organizadas, por la Asociación de Periodistas Europeos.

En este caso, tengo que añadir que, por vuestra parte, ha sido una **magnífica idea dedicar esta trigésimo segunda edición a las "Amenazas desde el Ciberespacio"**, que es uno de los espacios globales recogidos en la Estrategia de Seguridad Nacional de 2017 y, sin duda, uno de los ámbitos que más se ha visto afectado por la crisis del COVID.

Desde mi experiencia de mucho tiempo como miembro del Servicio de Inteligencia de España y, ahora, como su Directora, he podido comprobar la evolución de estas amenazas y su incremento muy significativo en los últimos años, y, sobre todo, **cómo la actual pandemia está acelerando esta tendencia**, al haberse ampliado el radio de acción de los ciberatancantes, su agresividad y la criticidad de los incidentes que protagonizan.

Estoy convencida de que durante las dos jornadas en las que se desarrollará este Seminario vamos a tener la oportunidad de reflexionar y de sacar conclusiones sobre estos riesgos cibernéticos que tocan de lleno a la seguridad nacional, la soberanía, el funcionamiento de las infraestructuras críticas, el patrimonio científico y tecnológico, la competitividad de nuestras empresas, la imagen exterior de España, o la privacidad de los datos de nuestros conciudadanos.

LA VELOCIDAD DEL CAMBIO. LA REVOLUCIÓN DIGITAL

Vivimos **un tiempo nuevo** que nos exigirá a todos un **gran esfuerzo** para estar en condiciones de aprovechar las enormes **oportunidades** que la tecnología nos ofrece y, a la vez, para hacer frente a los considerables **desafíos** que la revolución tecnológica está generando.

El **CNI**, como ya hiciera su antecesor, el **CESID**, ha desarrollado una **intensa actividad en este campo**. Más adelante me referiré a ello, a cuando a principios de los 80 un pequeño grupo de expertos del Servicio, verdaderos pioneros en la materia, comenzaron a estudiar y a prever las vulnerabilidades y los riesgos asociados al uso y aplicación de la tecnología de aquellos momentos. **De ahí venimos y ahí empezamos nuestra andadura en lo que ahora conocemos como "ciberespacio"**.

Es evidente que **lo que hace cuatro décadas nos parecía a casi todos ciencia-ficción**, hoy forma parte de nuestra vida cotidiana y **se ha convertido**, desde el punto de vista de la seguridad, **en una de las principales preocupaciones** de las Administraciones, de las empresas y de los propios ciudadanos; unas preocupaciones a abordar desde diferentes planos y con la colaboración de muchos y muy distintos actores.

Por esa razón, el **CNI es plenamente consciente de la necesidad de compartir encuentros como este con profesionales de los medios de comunicación**. Ustedes constituyen un muy buen vehículo para trasladar y hacer entender a la sociedad los riesgos a los que nos enfrentamos y para concienciarla sobre lo cada uno de nosotros podemos evitar mediante el uso responsable de las redes y sistemas de información y comunicaciones.

La relevancia de este asunto ya está siendo reconocida por los **medios y plataformas a las que Ustedes representan**, y cada vez es más frecuente encontrar en ellos secciones que comenzaron dedicadas a la tecnología, en general, y en las que progresivamente todo lo relacionado con **la ciberseguridad ha ido ganando mayor espacio**.

Oportunidades y desafíos son la cara y la cruz de una realidad innegable, que ya es presente y no un futurible; una realidad cambiante como pocas y que, además, avanza a una velocidad que nos obliga a una **actualización permanente** que, en el caso de los Servicios de Inteligencia,

se traduce en términos de recursos y, en concreto, de mejora de nuestras capacidades de prevención, detección, análisis y respuesta a las amenazas; una realidad, insisto, que nos impone una profunda **revisión de nuestros modelos de trabajo y de nuestras herramientas** para adecuarnos a ese "tiempo nuevo" al que antes me refería, al entorno digital en el que ahora todos nos movemos.

Déjenme decirles que a pesar de que en este foro nos vamos a centrar en las amenazas, es necesario empezar reconociendo que **el desarrollo tecnológico ha favorecido un período de auge económico y social sin precedentes**, y que puede ofrecer posibilidades de crecimiento al conjunto de la sociedad. Un cambio que tiene **impacto desde todos los ángulos** y que está modificando nuestro modo de vida, nuestra cultura, nuestras costumbres en general y nuestras estructuras sociales, que actualmente se desarrollan de manera paralela en el mundo físico y en el virtual.

Desde el punto de vista de los **Servicios de Inteligencia**, las nuevas tecnologías han creado un **entorno diferente que puede favorecer la consecución de los objetivos que perseguimos**, pero eso sí, **a cambio de que adaptemos**, como les acabo de señalar, **nuestro modelo de trabajo y los medios de los que nos servimos para realizarlo**. Nos enfrentamos a una verdadera sobreabundancia de información, que nos obliga a aumentar y modernizar nuestra capacidad para procesarla, tratarla, almacenarla, hacerla accesible, distribuirla y explotarla.

En otras palabras, el mundo digital en el que ya nos movemos nos exige enfoques novedosos, métodos distintos, instrumentos y técnicas más avanzadas y, en definitiva, **nuevas formas de hacer Inteligencia**, porque estamos determinados a que el CNI siga siéndole útil a los destinatarios del producto que elaboramos y continúe necesitándonos.

Aunque aún nos encontramos en el camino de esa renovación técnica, metodológica y procedimental, el horizonte que nos hemos marcado en cuanto a la integración de fuentes de datos, la fusión de información, la implantación de herramientas colaborativas y de sistemas de búsqueda global, la Inteligencia Artificial, etc., está suponiendo ya el **inicio de un cambio de mentalidad en el CNI**.

Se trata de un proceso similar al que también han emprendido nuestros homólogos del entorno europeo, y que nos está llevando a **pasar de un modelo basado tradicionalmente en la "necesidad de conocer" a otro en el que prima la "cultura de compartir"**, dentro del mantenimiento de los estándares de seguridad inherentes al trabajo de Inteligencia.

Este cambio tecnológico y de cultura corporativa afecta a todos los sectores de actividad del Servicio y, por lo tanto, es **perfectamente aplicable a cuanto hacemos en materia de ciberseguridad**.

Por eso, volvamos al ámbito ciber que es el que hoy nos ocupa, pero he creído oportuno **hacerles partícipes de la transformación a la que nos impulsan los avances tecnológicos**, de los que en el CNI somos usuarios y que, en este caso concreto, nos facilitan la tarea de identificar y tratar de neutralizar las amenazas procedentes del ciberespacio contra los intereses nacionales y la seguridad de los sectores público y privado y de los ciudadanos.

Pero no debemos olvidar que **esa revolución digital** que tanto nos favorece, porque nos abre nuevas y mejores posibilidades de actuación, **es la misma de la que se valen quienes crecientemente nos ciberatacan**: actores estatales, grupos organizados, colectivos de diversa índole e individuos aislados.

Unos **"enemigos sin rostro"**, como tantas veces les hemos definido, con capacidad para desarrollar acciones hostiles que, en cuestión de minutos, pueden comprometer los activos de cualquier organismo de la Administración, corporación, empresa, infraestructura, etc.; unos atacantes que **disponen de los medios y de la voluntad** de agredir los sistemas y las redes de cualquier objetivo público, privado o individual, que haya suscitado su interés para la consecución de sus **fines maliciosos**: el espionaje, la desestabilización, el robo, la extorsión o la suplantación de la identidad de personas físicas o jurídicas.

EL CENTRO CRIPTOLÓGICO NACIONAL

Para responder a este tipo de amenaza que era todavía emergente, porque su plasmación y sus efectos no se manifestaban aún con la virulencia actual, **en 2004 se creó el Centro Criptológico Nacional**, el CCN, que

como Ustedes saben está adscrito al CNI y cuyo personal se encuentra integrado orgánica y funcionalmente en el Centro Nacional de Inteligencia.

Como les decía al inicio de mi intervención -y hago un poco de historia-, el CCN tiene sus **orígenes** en una pequeña sección de nuestro antecesor, del CESID, que, a principios de la década de los 80, logró alcanzar un profundo conocimiento sobre las amenazas, vulnerabilidades y riesgos de los sistemas de información y comunicación de la época.

Antes he calificado a aquellos profesionales de **pioneros**, y lo fueron, pero lo cierto es que también tuvieron mucho de **visionarios** y trabajaron para hacernos comprender que la información que circulaba por medios electrónicos también debía ser protegida con medios *ad hoc* para impedir el acceso no autorizado de terceros, como tradicionalmente veníamos haciendo con la documentación en soporte papel y, en este caso, con medidas de seguridad física.

El paso del tiempo demostró que las amenazas eran reales, que había que estar preparados para hacerles frente y que la seguridad de redes y sistemas de información y, por lo tanto, del ciberespacio eran un reto que cada vez adquiría mayor prioridad. Y así quedó recogido en **2002**, en la **Ley reguladora del CNI**, que incorporó esta materia entre las funciones asignadas al Servicio que entonces se creaba.

Pero poco después dimos un paso más, o mejor dicho, el legislador dio un paso más, y **en 2004**, como acabo de comentarles, mediante un Real Decreto **se creó el CCN**, corroborando de esta forma la necesidad de contar con un **organismo específicamente encargado de la seguridad de los sistemas de información de la Administración**, y de garantizar la confidencialidad, la disponibilidad y la integridad de la información, incluida la información clasificada, que dichos sistemas procesan, almacenan o transmiten.

Después han venido otros, pero me van a permitir que señale, porque es un dato objetivo, que el CCN fue el **primer organismo constituido en España para ocuparse de la amenaza cibernética** y de la protección frente a ella.

En **2019** hemos celebrado el **décimo quinto aniversario de su creación** y, desde entonces, el Centro Criptológico Nacional se ha convertido en un **referente en su ámbito de actuación**, respetado y considerado dentro y fuera de nuestras fronteras. Así nos lo reconocen nuestros interlocutores nacionales y extranjeros y lo confirma el hecho de que por su experiencia, sus conocimientos técnicos y su eficacia, la intervención del CCN, su presencia y su colaboración son permanentemente solicitadas.

Les pongo **un ejemplo**: el CCN organiza anualmente las llamadas **Jornadas STIC**, que este año, en su décimo cuarta edición, se celebrarán del 30 de noviembre al 4 de diciembre. Estas Jornadas se han convertido en el principal encuentro de expertos de la ciberseguridad en español y en un referente en el panorama internacional. Congregan a toda la comunidad que interviene en la salvaguarda de nuestro ciberespacio: Gobierno, administraciones e instituciones públicas, empresas, universidades y ciudadanos. En 2019, las Jornadas STIC contaron con 130 ponentes, 60 empresas representadas y 3.500 asistentes.

Es decir, **el aumento del prestigio del CCN ha crecido en la misma proporción que el interés por la ciberseguridad**. A título anecdótico, pero ilustrativo, les confesaré que a las primeras Jornadas STIC, en 2007, acudieron 20 personas.

Durante sus 16 años de existencia, el CCN ha contribuido al fortalecimiento de la ciberseguridad nacional:

- protegiendo las redes y sistemas de organismos públicos y de entidades estratégicas,
- dando respuesta y gestionando incidentes y elaborando planes específicos para mitigar sus efectos,
- diseñando soluciones y herramientas de ciberseguridad,
- formando al personal de la Administración Pública y de las empresas,
- redactando guías, consejos y recomendaciones para difundir la cultura de ciberseguridad,
- contribuyendo a la generación de iniciativas tan relevantes como la creación del Centro de Operaciones de Ciberseguridad de la

Administración General del Estado, o la implantación del Esquema Nacional de Seguridad,

- promoviendo, en su calidad de organismo de certificación, el uso de productos y sistemas seguros, incluyendo los medios de cifra,
- colaborando en el desarrollo de estrategias y legislación,
- intercambiando información y técnicas con organismos homólogos de otros países, y
- representando a nuestro país en los foros y organizaciones multilaterales en los que la ciberseguridad ha adquirido un cada vez mayor protagonismo.

Todo este abanico de cuestiones relacionadas con la actuación del CCN está recogido en la **Memoria de Actividades** y en el **Informe sobre Ciberamenazas y Tendencias** que en estos próximos días haremos públicos. Les animo a que consulten ambos documentos si desean ampliar la información que les he proporcionado.

EL VALOR AÑADIDO DEL CNI

Y no me voy a extender más hablando del CCN, primero, porque no quiero interferir en la posterior intervención de su Subdirector, pero también, porque quiero centrarme en el valor añadido que aporta el CNI en su conjunto, y en el **tratamiento integral e integrado que hacemos de la ciberseguridad**.

En el Servicio de Inteligencia español, **bajo un mismo paraguas y con un mismo objetivo**, se coordinan los diferentes enfoques complementarios desde los que abordar la ciberseguridad. El trabajo del Centro en este ámbito incluye la **perspectiva técnica**, encomendada principalmente al CCN pero no solo a él, como luego veremos, y la dedicada al **análisis de Inteligencia** o Contrainteligencia tradicional, que se ocupa de las agresiones con origen en actores estatales dirigidas contra intereses españoles. Vamos a distinguir tres planos:

1. Por un lado, está la labor que desempeña el **CCN** y de la que acabo de hablarles, por lo que no voy a insistir en ello.

2. Por otro, y este es el enfoque puramente de **Inteligencia**, el CNI desarrolla una serie de líneas de acción que se resumen en la

investigación, el seguimiento y la valoración de las capacidades, las motivaciones y los objetivos de los agresores, y que se complementa con el análisis cualitativo de cada incidente para determinar qué tipo de información ha sido sustraída y qué consecuencias puede tener para la víctima.

Además, se lleva a cabo una labor de sensibilización sobre la amenaza que supone el ciberespionaje a cargo o patrocinado por potencias extranjeras, y sobre la necesidad de adoptar medidas para prevenir y neutralizar esos ataques. Esto se está haciendo tanto de manera proactiva, en organismos o en empresas que se considera que pueden ser de interés de terceros, como en aquellos que ya han sido objeto de agresión.

3. Por último, el Centro tiene también el recurso a la Inteligencia de Señales **(SIGINT)**, que es un elemento diferencial de nuestra actividad, en general, y, en este caso, de nuestra contribución a la ciberseguridad, dado que ningún otro organismo dispone ni de las capacidades técnicas, ni de las facultades legales para obtener, evaluar e interpretar el tráfico de señales de carácter estratégico, derivado de las comunicaciones internacionales, tal y como establece nuestra Ley reguladora.

Este acceso SIGINT a señales internacionales permite detectar agresiones y completa la labor técnica que realiza el CCN, en cuanto a análisis e investigación de ciberincidentes.

Esta combinación de enfoques y de capacidades de las que dispone el CNI constituye un **activo importante**. Nuestro conocimiento del mundo ciber es profundo, porque lo trabajamos desde ángulos distintos y, por eso, representa una potente herramienta para conseguir el mayor grado de certidumbre posible en la siempre complicada atribución de los ataques.

Como les decía, el tratamiento integral de las ciberagresiones, gracias a la **amplitud de competencias asignadas legalmente que nos confiere el hecho de ser Servicio de Inteligencia único de nivel nacional**, es lo que convierte en singular la aportación del CNI en este amplio mundo de la ciberseguridad en el que hoy, en este Seminario, nos hemos sumergido de la mano de la Asociación de Periodistas Europeos.

CIBERAGRESIÓN Y CIBERESPIONAJE

A ninguno se nos oculta que el ciberespacio permite operar con un alto grado de **impunidad y de anonimato** sobre todo tipo de objetivos, situados en cualquier lugar del mundo y desde no importa dónde; también todos somos conscientes de que tanto la **relación coste-eficacia** de las agresiones en ese entorno, como sus resultados son difícilmente alcanzables en comparación con el uso de otros medios.

Si a ello le unimos el hecho de que el mundo digital se caracteriza por la **ausencia de fronteras físicas** y que esta circunstancia hace que su ordenación normativa y jurisdiccional sea difícil de articular, tendremos el contexto casi perfecto para la ejecución de los ciberataques.

Con estas condiciones, **la ganancia de un agresor es enorme**, y más aún si se compara con el riesgo mínimo que corre. Quiero insistir en que los ciberatacantes, estatales o no, **mientras solo teman al fracaso, carecerán de motivos para dejar de intentarlo**, porque no pierden nada, porque prácticamente nunca sufren las consecuencias de sus actos.

Sabemos también que la **utilización de los avances tecnológicos** hace más efectivas y más complejas las agresiones desde el ciberespacio, y que esto incrementa el coste de las herramientas a usar en su contra.

Desde luego que no es mi intención pintar deliberadamente un panorama sombrío, pero esto es lo que tenemos, es la realidad a la que nos enfrentamos, no es un problema que podamos minimizar, y buena prueba de ello son las denominadas **amenazas persistentes avanzadas** (*Advanced Persistent Threat*, las APT por sus siglas en inglés), que agrupan las principales acciones ciberofensivas.

Detrás de cada APT existen grupos de trabajo estables, formados por equipos multidisciplinares, con altos conocimientos y gran cantidad de recursos materiales y económicos a su disposición, por lo que **suelen estar patrocinadas por Estados** o por grandes grupos cibercriminales. En el caso de los Estados, estos cuentan con unidades cíber especializadas en sus estructuras de inteligencia militares y civiles o con *proxies*, tales como

empresas tecnológicas, *hackers* o ciberdelincuentes, de los que se valen para ocultarse y ejecutar acciones ofensivas que no puedan ser fácilmente atribuidas.

De hecho, **la atribución de los ciberataques es cada vez más difícil**, debido a los grandes recursos técnicos y económicos que se destinan a la ocultación de su origen real.

España, tanto *per se* como por su pertenencia a organizaciones internacionales -especialmente la OTAN y la UE- con las que comparte intereses de todo tipo, continúa siendo objeto de constantes intentos de ciberataques por parte de actores estatales o de grupos esponsorizados por ellos, y no es previsible que esta tendencia deje de crecer en el futuro**.**

Con relación a nuestro país, los **objetivos prioritarios** continúan siendo, por un lado, la **Administración Pública**, buscando información sensible que le facilite posiciones de ventaja al agresor; y por otro, las **empresas de los sectores estratégicos** (energético, aeroespacial y defensa). Además, se ha observado un incremento de los ataques a las cadenas de suministro de las víctimas (intermediarios, proveedores, distribuidores, etc.), con redes habitualmente menos protegidas, como forma de acceso al objetivo final.

En el caso del **ciberespionaje económico**, no hay duda de que supone un grave y creciente riesgo para los intereses nacionales, puesto que su objetivo es el robo de la propiedad intelectual e industrial de empresas y organizaciones, y es **una actividad muy rentable**, porque, de tener éxito, le permite al agresor ahorrar tiempo y recursos en investigación científica y desarrollo tecnológico.

LOS EFECTOS DEL COVID-19

Y si hablamos de **crecimiento de los ciberataques y de las actividades de ciberespionaje**, no podemos obviar el hecho de que precisamente ese ha sido **uno de los efectos inmediatos del COVID-19**.

En líneas generales, la pandemia no ha sido un generador de nuevos riesgos o amenazas, sino un acelerador de tendencias existentes con anterioridad. Ha sido un **elemento indudablemente disruptivo e inesperado**, un **"cisne negro"**, según la terminología que hace años acuñaron los expertos para

referirse a un suceso improbable, que ocurre por sorpresa y que termina teniendo gran impacto. El COVID ha recuperado esta teoría, porque reúne todas las características que definen un caso de "cisne negro", aplicado en esta ocasión a la esfera política, económica, social, sanitaria, de seguridad…

Volvamos a nuestro ámbito y veamos cuáles han sido los **efectos de la pandemia** en el panorama de la ciberseguridad global, porque es evidente que ha influido, desde el momento en que la situación ha sido aprovechada por actores hostiles para potenciar sus ataques: desde las operaciones de robo de información, hasta las campañas de *ransomeware* o secuestro de datos.

Hace un par de días, leía en una publicación especializada que "alentados por la crisis sanitaria, el teletrabajo y el uso masivo de herramientas de colaboración digital (como la videoconferencia), han permitido a muchas empresas continuar su actividad". Aquí tenemos una de las claves para explicar el crecimiento de los ciberataques.

El hecho cierto es que el **uso obligado del teletrabajo** ha aumentado el área de exposición de los sistemas de información y de las redes, y el insuficiente nivel de seguridad en unos y en otras ha facilitado la entrada de los atacantes más agresivos y la actividad de grupos cibercriminales. La exposición no controlada de muchas organizaciones a Internet tiene este riesgo.

La tendencia va a continuar al alza y es previsible que los ataques y vulnerabilidades relacionados con redes domésticas o dispositivos personales se incrementen. El objetivo será acceder a la infraestructura de la institución o de la empresa del empleado que teletrabaja para conseguir distintos fines, entre los que el ciberespionaje será uno de los principales.

En general, el COVID-19 ha incrementado el riesgo de ciberataques, pero sobre todo lo ha hecho contra objetivos especialmente vulnerables y sensibles en estas circunstancias, como son **el sector sanitario, la industria farmacéutica y los centros de investigación**. La pugna por obtener la vacuna contra el virus y todo lo que implica su comercialización constituyen alicientes más que sobrados para que algunos actores, estatales o no, hayan emprendido una campaña de ataques especialmente virulenta.

Y claro está que **no solo en España se ha producido este fenómeno**. Con nuestros colegas de otros países occidentales hemos intercambiado información sobre las actividades de ciberespionaje que todos hemos sufrido sobre los organismos nacionales e instituciones involucradas en las investigaciones para desarrollar una vacuna contra el COVID-19.

El **CNI**, declarado por el Gobierno **"servicio esencial"** durante el estado de alarma, no ha bajado durante esos meses la guardia, y desde marzo hemos centrado nuestro **esfuerzo en garantizar la ciberseguridad del sector público español, y especialmente el sanitario**, precisamente en los momentos de mayor tensión de los servicios de salud, así como a detectar las actividades que pudieran afectar al tejido industrial y productivo.

Hemos observado un incremento cuantitativo de los ciberataques y un aumento cualitativo de su gravedad y hemos contrastado una mayor agresividad en la actuación de quienes utilizan el ciberespacio con fines maliciosos e ilícitos. Y, sobre todo, hemos empezado a ver cómo se va consolidando una tendencia que apunta a una **previsible disminución de las actividades "tradicionales" de espionaje, en favor de las "alternativas tecnológicas" representadas por el ciberespionaje**.

DESINFORMACIÓN

Pero **las posibilidades de utilización maliciosa del ciberespacio no se agotan con los ciberataques**, y las oportunidades de actuación que ofrece han favorecido que adquiera una relevancia inusitada un fenómeno tan antiguo como la desinformación.

En este caso, el ciberespacio es usado, no para ejecutar una agresión en sentido estricto, sino para **diseminar contenidos con una finalidad concreta**, recurriendo para ello a redes sociales, a medios de comunicación digitales y a programas informáticos, como es el caso de los *"bots"*, que automatizan y multiplican los mensajes.

Cuando la desinformación está dirigida a una determinada audiencia, durante un tiempo también determinado y con un objetivo definido, podemos hablar de **"campaña de desinformación"**. Y no se nos puede olvidar que lo que hay detrás de todo esto es una distorsión deliberada de la realidad (lo que ahora llamamos "postverdad"), **diseñada para modificar**

la opinión pública e influir a favor de los intereses del promotor de la campaña en cuestión, que normalmente se trata de una **potencia extranjera**, que se vale de ese instrumento para la consecución de objetivos poco o nada confesables.

Ahí está el peligro, en la voluntad de quien orquesta este tipo de acciones y lo hace para **desestabilizar, menoscabar la credibilidad de las instituciones, dañar la imagen y el prestigio de un país, polarizar a la sociedad o imponer relatos sesgados**, y siempre, como en el caso de los ciberataques, desde el anonimato.

Claro que no son una variante de las ciberagresiones, pero estas campañas comparten con ellas el aprovechamiento de las posibilidades que ofrecen el mundo virtual y los avances tecnológicos para ejecutarlas, como también comparten su eficiencia y la dificultad de su atribución. Pero, sobre todo, y por eso me interesa subrayar esta correlación: porque **ciberataques y desinformación son dos de las principales herramientas que se utilizan en el marco de las denominadas operaciones híbridas**.

Durante los últimos años, los procesos electorales habían sido uno de los objetivos principales de las campañas de desinformación. Sin embargo, a raíz de la crisis del COVID-19 algunos actores estatales han desarrollado una intensa actividad de desinformación a través del ciberespacio, poniendo de manifiesto el **poder disruptivo de la difusión de información manipulada y sus posibles consecuencias para la seguridad de los Estados**.

A lo largo de estos meses, el **CNI ha trabajado en la detección y el análisis de las campañas de desinformación originadas en el exterior** y difundidas a través de los aparatos de propaganda controlados o patrocinados por actores estatales, algunas de ellas muy agresivas en el planteamiento de narrativas anti-europeas.

En este período y en este contexto, el CCN ha elaborado y publicado una **Guía de Buenas Prácticas** frente a la desinformación; una Guía que tiene como principal destinatario al ciudadano, porque él es el objetivo, el receptor primordial del mensaje que trasladan estas campañas.

Además, hemos puesto en marcha el denominado **"observatorio ELISA"**, que es una herramienta diseñada por el propio CCN para analizar narrativas maliciosas y catalogar los medios que las difunden, y que entendemos que puede ser de utilidad para que nuestros conciudadanos conozcan la fiabilidad del origen de la información que reciben a través de las distintas plataformas.

Y una última reflexión por mi parte sobre este asunto, porque sé que mañana habrá una mesa dedicada monográficamente a él.

Con relación al fenómeno de la desinformación, se podría decir que **los Estados democráticos somos más vulnerables que los que no lo son**: y lo somos porque no censuramos los contenidos que circulan por redes sociales o difunden los medios de comunicación, ni controlamos el acceso a ellos; y porque no contamos con aparatos de propaganda que lancen campañas de esa naturaleza contra terceros. **A cambio**, eso sí, **tenemos libertad de expresión y de prensa**.

OPORTUNIDADES Y DESAFÍOS: UNA APUESTA POR LA COLABORACIÓN, EL COMPROMISO Y LA CONJUNCIÓN DE ESFUERZOS

Yo podía haber subtitulado mi intervención de hoy ante Ustedes con la frase **"oportunidades y desafíos"**, porque esta es una buena descripción de lo que representan la tecnología y el ciberespacio.

Hasta aquí, y desde la perspectiva de Inteligencia, les he hablado fundamentalmente de desafíos. Ahora, **quiero centrarme en las oportunidades**, que son, principalmente, las siguientes: la **sensibilización de la sociedad**, la **conjunción de esfuerzos a nivel nacional** de cuantos organismos tenemos competencias en el ámbito ciber, tanto en el sector público como en el privado, la **colaboración internacional** y la **acción concertada de los organismos multilaterales**.

Uno de los elementos esenciales a la hora de garantizar la seguridad en el ciberespacio es **el ciudadano**. Las personas pueden ser el motor que impulse la confianza en la tecnología, promoviendo procesos que la garanticen. Se trata de que el ciudadano sea consciente de los riesgos asociados al uso de la tecnología y que pueda exigir **que se incorpore la**

seguridad como un elemento de serie en los dispositivos y servicios que utiliza.

Para ello, empresas, fabricantes y proveedores de servicios, así como los responsables públicos y las Administraciones, incluido el CNI, debemos implicarnos para dar un salto cualitativo en la labor de **concienciación de los usuarios**, comprometiéndonos con la idea de que todos somos corresponsables de la ciberseguridad nacional y de que todos debemos hacer un uso responsable de las tecnologías.

Al hablar de los diferentes actores implicados en la sensibilización de la sociedad no he citado a **los medios de comunicación**, pero no porque me haya olvidado de ellos, de Ustedes, sino porque quiero hacer una mención especial al importante papel que juegan en ese empeño.

Y nada mejor que hacerlo en este foro, bajo el patrocinio de la Asociación de Periodistas Europeos.

No tengo ninguna duda de que **la participación activa de los medios en la concienciación de los ciudadanos es una baza de primer orden para elevar los niveles de ciberseguridad**. Ustedes, profesionales de la comunicación, representan una verdadera oportunidad en ese sentido, porque tienen una capacidad de llegar a la opinión pública, mayor que la que tenemos otras instancias. Contar con Ustedes para esta labor es una apuesta ganadora.

El resto de oportunidades que he mencionado tienen todas ellas un denominador común, que es la constatación de que **frente a amenazas globales como son las procedentes del ciberespacio, las respuestas deben ser también globales y basarse en la coordinación**. En la constatación de esa realidad, que nos conduce a una dinámica de cooperación entre organismos dentro y fuera de España y a la concertación de políticas y de normativa a nivel multilateral, reside una nada desdeñable oportunidad de éxito frente a quienes nos agreden.

Este es un problema al que nadie puede enfrentarse de forma aislada. Por eso, **la colaboración constituye un activo imprescindible** al que sería un error sustraernos. La conjunción de esfuerzos representa la mejor

oportunidad para afrontar los desafíos que nos plantea el uso malicioso del ciberespacio.

Y no duden de que el CNI participará activamente en ese esfuerzo para construir, entre todos, un entorno virtual seguro y confiable.

Muchas gracias de nuevo a la Asociación de Periodistas Europeos por su invitación y muchas gracias a todos Ustedes por su atención. Esta ha sido mi primera vez en este foro y confío en que no sea la última.

Les deseo a los organizadores de este Seminario, a los ponentes y a los asistentes que estos dos días sean fructíferos.

Muchas gracias.